

RDX 39

20101004kollbergasciil (2)

1

1 IN THE UNITED STATES DISTRICT COURT

2 DISTRICT OF MARYLAND

3 _____

4 Federal Trade Commission)

5 Plaintiff,)

6 v.) Civil No.

7 Innovative Marketing, Inc.,) RDB 08-CV-3233

8 Et al.)

9 Defendants.) JURY TRIAL DEMANDED

10 AND)

11 Maurice D'Souza)

12 Relief Defendant.)

13 _____)
Page 1

20101004kollbergasciil (2)

14

15 VIDEOTAPED DEPOSITION OF DIRK KOLLBERG

16 Hamburg, Germany

17 Monday, October 4, 2010

18 2:41 p.m.

19

20

21

22 REPORTED BY: FREDERICK WEISS, CSR, CM

□

2

1 Job No.: 2010-1004

2 Pages: 1 - 192

3 Videotaped deposition of Dirk Kollberg,

20101004kollbergasciil (2)
4 held at the offices of:

5

6

7 Marriott Armstrong Conference Room

8 Courtyard Hamburg Airport Hotel

9 Flughafenstrasse 47

10 22415 Hamburg, Germany

11

12

13

14 Pursuant to agreement, before Frederick

15 Weiss, Court Reporter.

16

17

18

19

20101004kollbergasciil (2)

20

21

22

□

3

1

A P P E A R A N C E S

2

ON BEHALF OF DEFENDANT KRISTY ROSS:

3

CAROLYN GURLAND, ESQUIRE

4

2731 N. Mildred Avenue,

5

Chicago, IL 60614

6

(312) 420-9263

7

E-mail: Cgurland@comcast.net

8

9

ON BEHALF OF THE FEDERAL TRADE COMMISSION

10

(By Skype and speakerphone)

20101004kollbergasciil (2)

11 COLLEEN B. ROBBINS, ESQUIRE

12 Federal Trade Commission

13 600 Pennsylvania Avenue, NW, Room 288

14 Washington, DC 20580

15 (202) 326-2548

16 E-mail: Crobbs@ftc.gov

17 ALSO PRESENT:

18 ANJA WEISS, AGCV, CCV, Videographer

19

20

21

22

□

20101004kollbergasciil (2)

2	EXAMINATION OF DIRK KOLLBERG	PAGE
3	Direct Examination by Ms. Gurland	6
4	Cross-Examination by Ms. Robbins	165
5	Re-Direct Examination by Ms. Gurland	187

6 ---o0o---

7 E X H I B I T S

8 (NO EXHIBITS WERE MARKED)

9

10

11

12

13

14

15

16

20101004kollbergasciil (2)

17

18

19

20

21

22

□

5

1

P R O C E E D I N G S

02:41:24 2

THE VIDEOGRAPHER: Today is Monday,

02:41:24 3

October the 4th, 2010. The time is 2:41 p.m.

02:41:32 4

This is Tape No. 1 of the video

02:41:34 5

deposition of Dirk Kollberg taken in the matter of

02:41:37 6

Federal Trade Commission, plaintiff, versus

02:41:39 7

Innovative Marketing, Inc., et al, defendants, and

20101004kollbergasciil (2)

02:41:44 8 Maurice D'Souza, relief defendant, in the United

02:41:47 9 States District Court, district of Maryland, Civil

02:41:54 10 Number RDB 08-CV-3233.

02:41:54 11 This deposition is taking place at

02:41:56 12 the Marriott Airport Hotel, Flughafenstrasse 47,

02:42:00 13 22415, Hamburg, Germany.

02:42:02 14 All persons will please identify

02:42:04 15 themselves for the record.

02:42:05 16 MS. GURLAND: On behalf of

02:42:07 17 defendant Kristy Ross, that's R-O-S-S, my name is

02:42:11 18 Carolyn Gurland, G-U-R-L-A-N-D.

02:42:15 19 MS. ROBBINS: On behalf of the

02:42:17 20 Federal Trade Commission, Colleen Robbins.

02:42:23 21 THE VIDEOGRAPHER: Will the court

02:42:30 22 reporter swear in the witness?

□

20101004kollbergasciil

03:10:28 20 Q. And -- but when you described what

03:10:30 21 -- what was being done at the beginning, you had

03:10:32 22 said -- you had used the pronoun "we."

□

32

03:10:34 1 Were -- were there other people

03:10:35 2 involved at the -- at the beginning of looking at

03:10:37 3 what was on the servers?

03:10:38 4 A. Yes, there was also a friend of

03:10:40 5 mine.

03:10:40 6 Q. And who was that?

03:10:41 7 A. He wants to stay anonymous. He

03:10:45 8 doesn't like to let his name known.

03:10:47 9 Q. Does he work at McAfee?

03:10:49 10 A. 20101004kollbergasciil
No.

03:10:50 11 Q. And you won't divulge -- you won't

03:10:54 12 say what the person's name was?

03:10:55 13 A. No. He doesn't like to. So I

03:10:58 14 respect this.

03:10:58 15 Q. Okay. In terms of the -- did you

03:11:09 16 let McAfee know what you were doing -- you and the

03:11:12 17 other individual, did you let them know about

03:11:15 18 everything you did, or were there things that you

03:11:17 19 did that McAfee didn't know about?

03:11:19 20 A. Well, the research was -- I told my

03:11:22 21 managers about the research I did and -- so yes,

03:11:29 22 with colleagues and then my managers.

□

20101004kollbergasciil

03:11:30 1 Q. what did you tell your managers

03:11:33 2 about the research that you did?

03:11:34 3 A. That we found web servers serving

03:11:38 4 the malicious files and that we found a way -- or

03:11:41 5 that I found a way to monitor those servers and to

03:11:45 6 download the latest creations of this fake IP.

03:11:50 7 So these files get updated a few

03:11:52 8 times a day, so it's always a different file. And

03:11:56 9 this is done to make it hard for antivirus

03:11:59 10 companies to keep up -- keep up with their

03:12:03 11 detection, so they have always to develop

03:12:05 12 something new.

03:12:05 13 Q. And were you copying from a long

03:12:10 14 period of time from November -- did you say -- the

03:12:13 15 time period, it started in November of 2008.

03:12:17 16 And when was the last time that you

20101004kollbergasciil

03:12:19 17 stopped copying material from these servers?

03:12:22 18 A. So these servers hosting the

03:12:29 19 malicious files, the server structure got changed

03:12:32 20 and we haven't been able to download files

03:12:35 21 anymore. And this change was in -- early in April

03:12:41 22 2009, I think.

□

34

03:12:48 1 Q. How did the structure change of the

03:12:50 2 -- of the servers? What was the difference?

03:12:54 3 A. The old servers have been hosting

03:12:57 4 status page where the IP address of someone who

03:13:02 5 was downloading the malicious files was included

03:13:04 6 and the path, the exact URI where the file is

03:13:09 7 located on the server.

20101004kollbergasciil

03:13:10 8 So I wrote an application to parse
03:13:15 9 the log file and take the download address and to
03:13:17 10 download the file again.

03:13:19 11 Q. okay. We might have to take that
03:13:20 12 in steps, if we can. Can we go back?

03:13:24 13 So you said that the -- the -- I
03:13:26 14 guess my original question was: How did the
03:13:29 15 behavior of the servers change in 2009 which
03:13:33 16 caused you to stop being able to download
03:13:36 17 information? So if we can just take it a step at
03:13:38 18 a time about what was different.

03:13:39 19 A. Yes. The servers which have been
03:13:42 20 downloading the software had a different software
03:13:45 21 running, a different web server application.

03:13:47 22 Q. The old servers?

□

20101004kollbergasci1

35

03:13:48 1 A. Well, those are different. The old
03:13:51 2 and the new. So they changed later to a different
03:13:53 3 server software, and then one was no longer
03:14:00 4 offering these report files that we've been
03:14:06 5 filing.

03:14:06 6 Q. Okay. So during the time period
03:14:08 7 that you were able to download information from
03:14:10 8 the server, can you just describe what you had
03:14:11 9 answered before to the question just so that I
03:14:14 10 could get each step down about what about it was
03:14:16 11 making it possible to get the information
03:14:19 12 downloaded somewhere else?

03:14:21 13 A. On the web servers which have been

20101004kollbergasciil

03:14:25 14 hosting the scareware, there was an HTML document,

03:14:32 15 like a log file showing the latest entries who has

03:14:38 16 -- who had downloaded the file from which location

03:14:41 17 on the server.

03:14:43 18 And I wrote an application to parse

03:14:46 19 those log files and to download the files again.

03:14:51 20 Those download URLs are only valid for 15 minutes,

03:14:54 21 so this program was running every 90 minutes to

03:14:58 22 see if new malware got hosted on the machines.

□

36

03:15:02 1 Q. So your application was an

03:15:05 2 application to download the log files from the

03:15:07 3 server?

03:15:09 4 A. A small -- yes, a small report,

20101004kollbergasci1

03:15:12 5 then to parse it, and to download the executable

03:15:15 6 files which were linked inside the log file.

03:15:22 7 Q. And then download the executables

03:15:24 8 that were?

03:15:26 9 A. The malicious files, the scareware.

03:15:28 10 Q. Right, but you said something else.

03:15:30 11 And then download the executables that were --

03:15:38 12 that were linked inside the log files?

03:15:40 13 A. Yes. That's correct, linked inside

03:15:43 14 the log files.

03:15:44 15 Q. And I think you -- you gave a

03:15:51 16 presentation, did you not, about your

03:15:53 17 investigation in connection with IMI.

03:15:55 18 Is that right?

03:15:56 19 A. Yes.

03:15:56 20 Q. Okay. And that was in Las Vegas?

20101004kollbergasciil

03:15:59 21 MS. ROBBINS: Carolyn, I'm sorry.

03:16:00 22 Could you have just repeat that one question? I
□

37

03:16:02 1 couldn't hear you.

03:16:02 2 MS. GURLAND: Yes. I said, "You

03:16:04 3 gave a presentation, did you not, about your

03:16:05 4 investigation of IMI?"

03:16:06 5 THE WITNESS: Yes.

03:16:07 6 BY MS. GURLAND:

03:16:07 7 Q. And that was in Las Vegas?

03:16:08 8 A. Yes, at McAfee Focus Conference.

03:16:11 9 Q. Was it -- was it a presentation

03:16:13 10 that you were doing on your own -- you know, on

20101004kollbergasciil
03:16:16 11 your own for yourself or were you doing the

03:16:18 12 presentation on behalf of McAfee?

03:16:20 13 A. It was my -- my research, but it

03:16:24 14 was presented during the McAfee conference, and

03:16:26 15 McAfee has been paying for -- for the trip. So

03:16:29 16 this was an official event.

03:16:31 17 Q. Okay. And you were there when you

03:16:33 18 gave the presentation as a representative of

03:16:35 19 McAfee --

03:16:36 20 A. Yes.

03:16:36 21 Q. -- is that fair to say?

03:16:37 22 When was that?

□

38

03:16:39 1 A. October of 2009, I think, maybe

20101004kollbergasciil

03:16:48 2 almost exactly the year.

03:16:49 3 Q. And --

03:16:51 4 A. It was the first day of the focus

03:16:54 5 conference last year.

03:16:55 6 Q. And what is a "focus conference"?

03:16:56 7 A. That's a customer conference or a

03:16:59 8 McAfee event in one of the big conference halls in

03:17:07 9 Las Vegas, and we're presenting about new trends

03:17:10 10 on the web and where -- where do we see the big

03:17:13 11 problems in the future, how does the threat

03:17:15 12 landscape change, presentation about products and

03:17:22 13 partners are there as well.

03:17:22 14 THE REPORTER: Products and who?

03:17:22 15 THE WITNESS: Partners.

03:17:23 16 BY MS. GURLAND:

03:17:23 17 Q. And what was the topic on which you

20101004kollbergasci1

03:17:27 18 presented personally?

03:17:28 19 A. There was on -- yeah. What was the

03:17:33 20 title? Inside the scareware company.

03:17:38 21 Q. And the company that you were

03:17:39 22 talking about is IMI.

□

39

03:17:40 1 Is that right?

03:17:42 2 A. Innovative Marketing, yes.

03:17:44 3 Q. Innovative Marketing, right.

03:17:46 4 Was there a fee for the people who

03:17:48 5 came to the conference, do you know?

03:17:49 6 A. No, I don't know.

03:17:50 7 Q. You don't know?

03:17:51 8 A. No.

20101004kollbergasciil

03:17:53 9 Q. Okay.

03:17:54 10 A. That's --

03:17:55 11 Q. Okay. Did you get a fee for

03:17:57 12 speaking at the conference?

03:17:58 13 A. No.

03:17:58 14 Q. But you were employed by McAfee at

03:18:01 15 the time.

03:18:02 16 Is that right?

03:18:02 17 A. Yes.

03:18:02 18 Q. And so you were, during that period

03:18:04 19 of time, making your regular salary from McAfee --

03:18:09 20 A. Yes.

03:18:09 21 Q. -- right?

03:18:10 22 A. But I'm -- I'm not allowed to work

□

20101004kollbergasciil

03:18:12 1 in the US, so I don't have a work permission,

03:18:15 2 so...

03:18:15 3 Q. Don't worry. That's not where I

03:18:17 4 was going.

03:18:18 5 But was -- but was it part of your

03:18:19 6 job? I mean, you did this in connection with your

03:18:21 7 job that you held at McAfee?

03:18:23 8 Is that right?

03:18:23 9 A. Yes.

03:18:23 10 Q. All right. And in terms of the

03:18:27 11 presentation that you gave, I think -- and I can

03:18:32 12 at various -- represent to you that I have various

03:18:34 13 articles. I'm not going to introduce them at this

03:18:36 14 time.

20101004kollbergasciil

03:18:36 15 But it was, anyway, my impression

03:18:39 16 from the articles that the -- that the description

03:18:43 17 of accessing the servers, the description included

03:18:50 18 the observation that there -- that there was a

03:18:57 19 security vulnerability on the servers?

03:19:00 20 A. No. I haven't made use of any

03:19:03 21 vulnerabilities, no.

03:19:06 22 Q. okay.

□

41

03:19:07 1 A. That's not allowed in Germany. so

03:19:09 2 even if they have been dialogues asking for

03:19:13 3 username and password, we have stopped and we

03:19:16 4 haven't tried any default passwords or anything.

03:19:19 5 So all the information are just

20101004kollbergasciil

03:19:20 6 completely free on the web without any username

03:19:23 7 and password certification, without any tricks or

03:19:27 8 injections or code injections or anything.

03:19:27 9 THE REPORTER: (Interruption)

03:19:27 10 THE WITNESS: Injections -- code

03:19:27 11 injections.

03:19:35 12 BY MS. GURLAND:

03:19:35 13 Q. Okay. So would it be accurate to

03:20:12 14 -- so would it be accurate or inaccurate to

03:20:13 15 describe that during the time that you found the

03:20:18 16 servers, that you were surprised that the servers

03:20:21 17 were not passware protected -- password-protected.

03:20:27 18 Is that right?

03:20:27 19 A. For normal coding, I would expect

03:20:30 20 to have internal servers not connected to the

03:20:33 21 internet. I don't know why they made the decision

20101004kollbergasciil

03:20:35 22 to connect to the internet, maybe for remote

□

42

03:20:38 1 people to connect. But even then, usually I would

03:20:42 2 suggest to password-protect those systems, yes.

03:20:45 3 Q. Okay. And would it be accurate to

03:20:47 4 describe the way that the servers were set up as a

03:20:51 5 security lapse of breathtaking irony? Was it a

03:20:55 6 security lapse the way that the servers were set

03:20:58 7 up? Would you describe it like that?

03:21:00 8 A. Not necessarily, no. We -- based

03:21:08 9 on the information that we found, they had an

03:21:12 10 internal VPN network, so they know how to secure

03:21:16 11 their systems. But, again, I don't know for which

03:21:18 12 20101004kollbergasciil
reason they decided for put some on the internet

03:21:22 13 directly. As I don't know the reasons, I can't

03:21:25 14 tell if this was by mistake or if it served some

03:21:32 15 purpose.

03:21:38 16 Q. And what types of material -- well,

03:21:43 17 first of all, you had said that there was just not

03:21:46 18 one server but more than one server.

03:21:48 19 Is that right?

03:21:49 20 A. Yes.

03:21:49 21 Q. Can you -- how many servers were

03:21:52 22 there?

□

43

03:21:52 1 A. I think we had about 38 servers

03:21:56 2 hosting the malware and 18 other servers which we

20101004kollbergasciil

03:22:05 3 found or which might be related to Innovative

03:22:10 4 Marketing.

03:22:10 5 So, for example, we found the

03:22:13 6 external code server -- external call center, they

03:22:17 7 have been recalling all their customer calls, and

03:22:19 8 those have been published on the web as well.

03:22:23 9 Q. And is the external call center,

03:22:25 10 was that information that was contained on one

03:22:29 11 server?

03:22:29 12 A. Yes.

03:22:30 13 Q. Was there other information on that

03:22:33 14 same server or was there just one server that was

03:22:36 15 devoted to external call center information only?

03:22:41 16 A. So these servers have not been in

03:22:47 17 the IP range of Innovative Marketing Ukraine.

03:22:50 18 This was outside, but they had -- but when you

20101004kollbergasciil

03:22:54 19 listen to the calls, they are supporting the

03:22:57 20 products from Innovative Marketing.

03:22:58 21 Q. And did you listen to the calls?

03:23:04 22 A. I listened to a few, yes.

□

44

03:23:06 1 Q. And was it -- in what form were

03:23:08 2 they captured?

03:23:09 3 A. Audio files, so some as wav files

03:23:11 4 some as GSM files.

03:23:13 5 Q. And did you listen to just some of

03:23:15 6 them or all of them?

03:23:16 7 A. Just some. It's too many.

03:23:18 8 Q. And is it -- is it accurate to say

03:23:20 9 that -- that a surprising thing was that 95

20101004kollbergasciil

03:34:43 18 Q. okay. well, is it -- I guess what

03:34:46 19 I'm trying to get at, is it generic or is it

03:34:49 20 something that was one -- could more than one

03:34:52 21 company use it?

03:34:53 22 A. This is something that more people

□

56

03:34:57 1 have been using, not only -- not only one company.

03:35:00 2 Q. And was there a particular version

03:35:03 3 or, you know, a particular thing about this

03:35:07 4 toolkit that made it unique? Did it have a number

03:35:09 5 or a way to look it up to know that there is one

03:35:13 6 particular one or it's just a generic kind of

03:35:17 7 tool?

03:35:17 8 A. The GNIDA was especially created to

20101004kollbergasciil

03:35:21 9 exploit a vulnerability in the Adobe Shockwave

03:35:21 10 Player.

03:35:21 11 Q. Okay. I'm not sure that answer --

03:35:25 12 is it unique? Is it -- can you uniquely identify

03:35:28 13 the toolkit? Is there a serial number or

03:35:31 14 registration number or hash value or anything of

03:35:34 15 that nature?

03:35:34 16 A. There is some GUI interface, and

03:35:39 17 you can look at the README.TXT file. So you see,

03:35:42 18 there are many files that belong to this toolkit.

03:35:45 19 So...

03:35:45 20 Q. Do you have any idea who

03:35:48 21 particularly, either a corporation or an

03:35:49 22 individual, developed this toolkit?

□

20101004kollbergasciil

03:35:51 1 A. No, I don't.

03:35:52 2 Q. Did you ever try to contact anybody

03:35:57 3 from Innovative Marketing at the point in time

03:36:00 4 that you learned that there was some ability to

03:36:03 5 get information from servers registered to this

03:36:07 6 entity?

03:36:07 7 A. No, I didn't.

03:36:08 8 Q. So no correspondence with anybody

03:36:12 9 of any sort?

03:36:13 10 A. No.

03:36:13 11 Q. You were describing before the way

03:36:20 12 that the -- the way that you were able to get to

03:36:25 13 the information that was on the server?

03:36:26 14 A. Yes.

03:36:27 15 20101004kollbergasciil
Q. Okay. And just so I understand,

03:36:29 16 the server was -- how -- how did it work that it

03:36:34 17 was connected to the internet that -- that -- was

03:36:38 18 it on a -- was it a link that you could

03:36:40 19 immediately go from a company web site immediately

03:36:44 20 to this server?

03:36:45 21 A. No. This was you just enter the IP

03:36:49 22 address in the -- in your web browser and press
□

58

03:36:53 1 return, and then it took us to the page.

03:36:56 2 Q. And what happened after it took you

03:36:58 3 to the page?

03:36:59 4 A. It was displaying the -- its

03:37:03 5 contents. That's what a web server is supposed to

20101004kollbergasciil

03:37:06 6 do.

03:37:06 7 Q. So it took you to a page, and on

03:37:09 8 this page was displayed the contents of the server

03:37:11 9 immediately?

03:37:12 10 A. There have been interfaces and --

03:37:15 11 like a wiki page where you can click through.

03:37:25 12 Q. what would a person have to do to

03:37:27 13 get from the IP address to the page -- the IP

03:37:32 14 address, if you go to the -- on the web browser

03:37:35 15 and look at a page, what would a person have to do

03:37:37 16 to get from there to the information on the

03:37:40 17 server? what were all the steps that a person

03:37:42 18 would have to take?

03:37:43 19 A. Just to enter the IP address and to

03:37:45 20 press return.

03:37:46 21 Q. And that -- but that just takes to

20101004kollbergasciil

03:37:49 22 a page, that doesn't take you -- well, where does

□

59

03:37:52 1 it take you exactly?

03:37:53 2 A. To the server.

03:37:53 3 Q. To the server?

03:37:54 4 A. To the web server for the IP.

03:38:00 5 Q. And once you were on the web

03:38:02 6 server, was it immediately possible to get all of

03:38:06 7 the information on that server?

03:38:08 8 A. Yes.

03:38:09 9 Q. And how exactly does that -- does

03:38:12 10 that work? Did it display -- well, how many --

03:38:15 11 how much information are we talking about? I

03:38:19 12 mean, is this the 63 gigabytes of information or

20101004kollbergasciil

03:38:22 13 is that the aggregate of all the different

03:38:24 14 servers?

03:38:25 15 A. It's all together --

03:38:25 16 Q. Okay.

03:38:26 17 A. -- so a part of that.

03:38:28 18 Q. Okay. So let's -- let's take --

03:38:29 19 let's take -- let's assume that we are dealing

03:38:31 20 with one of the eight servers that was registered

03:38:33 21 to IMI. Let's take that for a minute. So we're

03:38:37 22 in -- we're in -- we have gone to the IP address;

□

60

03:38:39 1 we're in a web browser -- I mean, the web browser

03:38:44 2 has taken us to a page.

20101004kollbergasciil
And then what -- and then what --

03:38:45 3

03:38:49 4 what's displayed -- what is displayed for the user

03:38:53 5 to see once the user does what you say and clicks

03:38:56 6 on something?

03:38:56 7 A. So, for example, the Asterisk phone

03:39:01 8 system was showing the Asterisk welcome screen,

03:39:04 9 and from there you have a menu where you can click

03:39:07 10 and see statistics and go through the menus.

03:39:16 11 Q. When you say that you could see the

03:39:18 12 menus, could you -- was there sort of a directory

03:39:21 13 when you went into this about all the information

03:39:24 14 that would be contained on that server?

03:39:25 15 A. Yes.

03:39:27 16 Q. And you would -- would it display

03:39:31 17 the directory and then when you clicked on one of

03:39:35 18 the line items that you were interested in, it

20101004kollbergasciil

03:39:37 19 would take you there? Is that how it worked?

03:39:40 20 A. It's like when you -- when you are

03:39:44 21 in a normal web site and there is like a news

03:39:47 22 magazine and there is a link to another story, and

□

61

03:39:49 1 so there is a link that you click on.

03:39:51 2 And then it takes you to the next

03:39:55 3 page, and there was one button for the people

03:39:57 4 directory, for example, and then we saw 666

03:40:01 5 entries of people working for this company and --

03:40:07 6 Q. What kind of information was

03:40:09 7 available on the servers about the people who

03:40:13 8 worked for the company?

03:40:14 9 A. A lot of -- many documents had

20101004kollbergasciil

03:40:18 10 names inside of who has lost one, who modified the

03:40:25 11 document or who created it.

03:40:26 12 Q. Are these the log files that you

03:40:27 13 were talking about?

03:40:28 14 A. No, these were just the documents

03:40:29 15 on the web server in the --

03:40:34 16 Q. Okay.

03:40:34 17 A. And --

03:40:35 18 Q. Any information about the

03:40:36 19 individuals specifically?

03:40:36 20 A. There has been the phone book that

03:40:41 21 some people had their private E-mail addresses in

03:40:44 22 that, pictures of themselves or some other

□

20101004kollbergasci1

04:14:58 14 in the US, who you don't remember who they are or

04:15:01 15 what they said, did you talk to Mr. Schmidt again

04:15:04 16 after that?

04:15:05 17 A. No.

04:15:05 18 Q. And do you remember anything that

04:15:11 19 you were -- that -- anything you changed about

04:15:14 20 your presentation after talking to Mr. Schmidt or

04:15:17 21 the lawyer who you don't remember?

04:15:18 22 A. No.

□

99

04:15:22 1 Q. So you don't remember any -- do you

04:15:25 2 remember anything at all about -- about those

04:15:26 3 contacts with lawyers, about the presentation?

04:15:31 4 A. No. I was really busy at the end,

20101004kollbergasciil

04:15:33 5 because I had to change the presentation and get a
04:15:36 6 new layout on, because McAfee templates changed,
04:15:40 7 and this was taking a lot of time to change the
04:15:43 8 presentation, the framework.

04:15:44 9 Q. And the reason that you just said
04:15:46 10 is because McAfee templates changed? Is that why
04:15:50 11 you had to change it?

04:15:51 12 A. No. That -- that made the time
04:15:54 13 before the presentation quite busy for me. I
04:16:02 14 don't really -- I can't exactly recall when I've
04:16:05 15 been talking to him.

04:16:06 16 Q. Okay. And do you remember anything
04:16:07 17 about the presentation at all that you changed
04:16:10 18 based on conversation with lawyers?

04:16:12 19 A. No, there wasn't anything.

04:16:13 20 Q. Other than the conversation that --

20101004kollbergasciil

04:16:29 21 with Mr. Schmidt and then those other lawyers in

04:16:31 22 the US, and other than the conversation that you
□

100

04:16:34 1 had with McAfee lawyers about the procedure about

04:16:40 2 delivering the hard drive to the FTC, do you

04:16:43 3 remember any other conversations with lawyers in

04:16:47 4 this matter at any time?

04:16:49 5 A. No.

04:16:50 6 Q. How many conversations do you

04:16:53 7 recall with lawyers about the actions that you

04:16:55 8 took gathering data from the servers?

04:16:58 9 A. It might have been three or four,

04:17:06 10 four calls, five calls, I don't know.

04:17:08 11 20101004kollbergasciil
 Q. Based on any of the information

04:17:12 12 that you received from the lawyers in these calls,

04:17:17 13 approximately five or you don't know, did you ever

04:17:20 14 seek to consult a lawyer who was representing just

04:17:24 15 you personally?

04:17:24 16 A. No.

04:17:25 17 Q. Now, when you were discussing the

04:17:33 18 issue of the information on the IMI servers being

04:17:37 19 available to the public, is that what you -- is

04:17:40 20 that what your position is, it was available to

04:17:42 21 the public?

04:17:42 22 A. Yes. The server was connected to
□

101

04:17:44 1 the web -- to the internet, yes.

20101004kollbergasciil

04:17:48 2 Q. Okay. Does that mean that -- what

04:17:50 3 -- what type of special technical know-how would a

04:17:54 4 person have to have -- during the time that you

04:17:57 5 say that that server was connected to the web

04:18:00 6 site, what kind of technical know-how, if any,

04:18:04 7 would a person have to have to get on to the

04:18:06 8 content of that server?

04:18:07 9 A. He would need a web browser and to

04:18:09 10 put in the IP address of one of Innovative

04:18:14 11 Marketing's marketing's IP -- IPs they had.

04:18:18 12 Q. Is that all that you would need?

04:18:19 13 A. Yes.

04:18:20 14 Q. Would -- so is it fair to say that

04:18:22 15 a person wouldn't need any specialized technical

04:18:25 16 know-how to access the server at the time that you

04:18:27 17 did?

20101004kollbergasciil

04:18:27 18 A. Yes.

04:18:27 19 Q. And if a person could access the

04:18:31 20 server, would it be fair to say that they could

04:18:33 21 also access files that were on the server?

04:18:35 22 A. This was a web server serving web

□

102

04:18:40 1 pages. Some of them, there have been others, I

04:18:47 2 don't know which -- so the web server, the big

04:18:54 3 one, that one, yeah, was -- was like a web front

04:18:57 4 end that you can navigate through, and it's

04:18:59 5 dynamically building the content that you request.

04:19:05 6 Q. Okay.

04:19:06 7 A. Like there is a fixed header line;

04:19:08 8 there is a fixed bottom line.

20101004kollbergasciil

04:19:10 9 Q. Okay. And is it possible to access

04:19:12 10 particular files on the -- on the server once you

04:19:15 11 can get in there?

04:19:16 12 A. what do you mean with "files"?

04:19:19 13 Q. They are not particular files? I

04:19:22 14 guess the -- take for example the roster of the

04:19:26 15 666 employees, in what format is that? Is that

04:19:30 16 not a file --

04:19:30 17 A. That's --

04:19:31 18 Q. -- and/or a document?

04:19:32 19 A. Yes. If you like, it's an HTML

04:19:37 20 document which gets dynamically created by the web

04:19:42 21 server which reads from some database on the hard

04:19:45 22 disk and transfers this as an HTML page to the web

□

20101004kollbergasciil

04:19:49 1 client.

04:19:49 2 Q. Okay. So is it possible if you can

04:19:51 3 access that HTML page, could you -- I'm not saying

04:19:58 4 that you did this, but could you, if you're in

04:20:00 5 there, could you do -- make any kind of change to

04:20:02 6 that page once you're in there? Is it possible?

04:20:07 7 A. I don't know. I have no clue. So

04:20:10 8 I don't know if you have to log in to make changes

04:20:13 9 to documents, if you have to -- so the people who

04:20:18 10 created the documents, there was a name included

04:20:19 11 in the pages. And I don't know if they have to

04:20:22 12 authenticate themselves to do modifications. That

04:20:27 13 was none of my interest.

04:20:28 14 Q. Okay. But based on your -- without

20101004kollbergasciil

04:20:32 15 -- and I appreciate that your testimony is that

04:20:34 16 you didn't try to do anything to the pages that

04:20:37 17 you saw.

04:20:38 18 But do you have any information to

04:20:39 19 offer just based on your technical expertise, as

04:20:43 20 to whether or not based on what was going on,

04:20:46 21 based on the setup that you're describing, whether

04:20:48 22 or not it's possible to make changes?

□

104

04:20:50 1 A. I don't know. I can't tell. I

04:20:54 2 don't know this application in detail. I don't

04:20:55 3 know how it was set up.

04:20:58 4 Q. Okay. So you don't know one way or

04:21:00 5 another whether or not you can?

20101004kollbergasciil

04:21:03 6 A. Yes.

04:21:04 7 Q. So it's fair to say that you didn't

04:21:08 8 -- it wasn't -- you didn't need software to

04:21:10 9 download any data from the -- from the server?

04:21:14 10 Was it -- was it a process that you used software

04:21:16 11 to do or not?

04:21:17 12 A. Yeah, you can do it if you do it on

04:21:19 13 the web server and type the IP address and then go

04:21:23 14 on file, save as, or I've been using wget. This

04:21:27 15 is an online tool.

04:21:28 16 Q. Using -- okay. So this is -- now,

04:21:32 17 just so that we are clear, this is a tool that

04:21:34 18 during the time period from November 2008 through

04:21:36 19 April of 2008, when you were pulling information

04:21:39 20 from the server?

04:21:41 21 A. Yeah.

20101004kollbergasciil

04:21:42 22 Q. Okay. I'm asking you about what
□

105

04:21:44 1 the -- what software tool, if any, you used to do

04:21:46 2 that?

04:21:47 3 A. That was wget to take mirrors of

04:21:53 4 the server.

04:21:53 5 THE REPORTER: (Interruption)

04:21:53 6 THE WITNESS: wget.

04:21:55 7 BY MS. GURLAND:

04:21:55 8 Q. W-G-E-T?

04:21:56 9 A. Yes.

04:21:57 10 Q. And then take, T-A-K-E?

04:21:59 11 A. No. Just wget.xe.

04:22:02 12 Q. 20101004kollbergasciil
And what is that?

04:22:03 13 A. That's an online application that
04:22:06 14 you can give an IP address and some parameters,
04:22:09 15 and then it starts connecting to the web server
04:22:13 16 like a web browser does, and it downloads files
04:22:17 17 found on the server.

04:22:18 18 Q. Can you back up to that, give the
04:22:22 19 IP address in parameters and then it does?

04:22:25 20 A. Then connects to the web server and
04:22:27 21 downloads the files.

04:22:33 22 Q. Was there ever any problem
□

106

04:22:38 1 downloading the information from the server?

04:22:40 2 A. No.

20101004kollbergasciil

04:22:41 3 Q. It didn't ever pause, stop or have

04:22:44 4 an error message and not be able to do it, or

04:22:47 5 every single time it just downloaded it right

04:22:50 6 away?

04:22:50 7 A. The script was set to do

04:22:52 8 incremental updates, which means I was running it

04:22:58 9 once and the next week again, and then it was

04:23:01 10 checking if any content on the web server changed

04:23:04 11 in the mean time and if it was updating the

04:23:07 12 content of the local mirror that I had.

04:23:09 13 Q. So in the last part, and if it was?

04:23:13 14 A. If it was different than it was

04:23:19 15 storing the newer version on -- on the local copy.

04:23:22 16 Q. And when it stored the newer

04:23:23 17 version, would it overwrite the older version?

04:23:25 18 A. Yes.

20101004kollbergasci1

04:23:27 19 Q. Is the information about when the
04:23:36 20 newest version of each of the pieces of
04:23:39 21 information that was added to the -- I guess to
04:23:43 22 the hard drive ultimately, is that -- can one tell
□

107

04:23:46 1 from having those files when -- when the last
04:23:50 2 piece of information was added?
04:23:51 3 A. Some documents had time stamps in,
04:23:56 4 so it was saying like someone edited the file at
04:24:00 5 this date, this time, but this is not for all
04:24:05 6 files.

04:24:06 7 Q. And the time stamp, what would the
04:24:10 8 time stamp reflect? would it reflect when it went
04:24:13 9 from the server to the -- to the hard drive that
Page 169

20101004kollbergasciil

04:24:16 10 you had?

04:24:16 11 A. No. It was when the document

04:24:18 12 changed on the web server.

04:24:19 13 Q. Oh, okay. So in terms of the --

04:24:30 14 the -- when one looks at the content of the 63 or

04:24:34 15 67 gigabytes of material that's on the hard drive,

04:24:37 16 can one tell for any individual, can I say file,

04:24:42 17 any individual file, when it was added to the

04:24:46 18 server -- I mean, when it was added to the hard

04:24:49 19 drive?

04:24:49 20 A. Yes. The time stamps of the files

04:24:52 21 are accurate on the hard drive.

04:24:53 22 Q. Okay. And will those time

□

20101004kollbergasciil

04:24:55 1 stamps -- is it accurate to say that those time

04:24:59 2 stamps would reflect the -- the point in time when

04:25:01 3 it was taken from the -- from the server and

04:25:03 4 stored on to the hard drive?

04:25:04 5 A. Yes.

04:25:05 6 Q. Okay. Did you use -- did you use

04:25:23 7 the EnCase tool to store the files? when you

04:25:27 8 finished compiling the 63 gigabytes of

04:25:35 9 information, did you put it into an EnCase format

04:25:38 10 yourself?

04:25:38 11 A. I don't know what EnCase is.

04:25:39 12 Q. So I guess the answer is that you

04:25:41 13 didn't?

04:25:41 14 A. No.

04:25:41 15 Q. Did you put it in -- did you do

20101004kollbergasciil

04:25:42 16 anything to that data before sending it off to the

04:25:46 17 -- I guess the first -- the first was the German

04:25:48 18 LKA.

04:25:49 19 Did you do anything to put the data

04:25:52 20 in any form before you sent it?

04:25:55 21 A. I put them into a TrueCrypt volume.

04:25:58 22 Q. Into a?

□

109

04:26:00 1 A. TrueCrypt.

04:26:01 2 Q. TrueCrypt.

04:26:03 3 And that was a -- that was

04:26:05 4 password-protected?

04:26:06 5 A. Yes.

04:26:06 6 Q. Is that what's that's about? And

20101004kollbergasci1

04:26:08 7 then did you give LKA in Hamburg the password, is

04:26:12 8 that how it works?

04:26:13 9 A. Yes.

04:26:13 10 Q. And did you just, like, walk over

04:26:15 11 with it --

04:26:15 12 A. Yes.

04:26:15 13 Q. -- or drive over with the -- with

04:26:17 14 the physical hard drive?

04:26:17 15 A. Yes.

04:26:18 16 Q. Okay. After you delivered that to

04:26:20 17 the LKA in Hamburg, have you had any follow-up

04:26:24 18 conversations with them? Did they ask anything

04:26:26 19 else of you after that?

04:26:27 20 A. No.

04:26:28 21 Q. Did they ask any follow-up

04:26:30 22 questions about what they were looking at or how

20101004kollbergasciil

□

110

04:26:33 1 -- how you got it or what happened?

04:26:34 2 A. I met them again, I think, half a

04:26:39 3 year later, but they haven't done any

04:26:42 4 investigations, because they had no open case at

04:26:45 5 that time.

04:26:45 6 Q. Did you tell them about the -- the

04:26:51 7 FTC, that your contacts with the FTC to let them

04:26:57 8 know that there was another case?

04:26:58 9 A. Yes. Yes.

04:26:59 10 Q. Okay. And what -- what was that

04:27:00 11 conversation, as much as you remember? First of

04:27:03 12 all, is there an individual at the LKA in Hamburg

05:37:41 21 20101004kollbergasciil
Q. That you can think of, that's a

05:37:43 22 good reason to do that, is there any good reason
□

151

05:37:45 1 that you can think of to do that?

05:37:47 2 A. Well, to give remote access to

05:37:49 3 other people.

05:37:49 4 Q. Okay. But is there not an ability

05:37:51 5 to give remote access to other people that can be

05:37:54 6 set up without giving access to audio files of

05:37:56 7 customer complaints to everybody with a computer?

05:37:58 8 MS. ROBBINS: Objection. He's

05:37:59 9 already testified that there may be reasons, and

05:38:01 10 he doesn't know what they are.

05:38:05 11 THE WITNESS: So I think --

20101004kollbergasciil

05:38:06 12 BY MS. GURLAND:

05:38:06 13 Q. Same question. Well, you said

05:38:08 14 there may be reasons, and I just -- well, this is

05:38:10 15 a more specific question, because you had said in

05:38:13 16 answer to something that I said, you said because

05:38:15 17 you wanted -- you said as an example of a reason,

05:38:18 18 because in fact you can testify to such things,

05:38:21 19 you said that maybe it was the case that they

05:38:22 20 wanted to, you know, give a link to someone in the

05:38:25 21 call center.

05:38:25 22 But -- but that's -- but I'm asking

□

152

05:38:27 1 something about -- I mean, couldn't you do that

05:38:29 2 without -- if you wanted to do something like

20101004kollbergasci1

05:38:31 3 that, the example that you gave me, couldn't you
05:38:32 4 do that without giving access to everybody in the
05:38:35 5 world with a computer? As a technical matter, is
05:38:37 6 it possible?

05:38:38 7 A. There are different methods to do
05:38:39 8 that, yes.

05:38:40 9 Q. Okay.

05:38:41 10 A. But I don't know need -- don't know
05:38:42 11 the need or the intention behind it. So it
05:38:45 12 depends on -- on what you're going to set up.

05:38:47 13 Q. Okay. But -- but it's your
05:38:49 14 testimony that records of customers complaining
05:38:52 15 about the software were on the internet for
05:38:56 16 anybody with a computer to listen to and -- and
05:38:59 17 get to.

05:39:00 18 Is that right?
Page 241

20101004kollbergasci1

05:39:00 19 A. Yes.

05:39:00 20 Q. And you had also told me earlier

05:39:03 21 that it was -- it was set up like that, that a

05:39:05 22 person didn't even have to have any kind of

□

153

05:39:08 1 technical expertise of any sort to -- to -- to get

05:39:11 2 right into that and listen -- to get right into

05:39:13 3 those audio files and listen to the complaints.

05:39:16 4 Is that right?

05:39:16 5 A. Yes.

05:39:18 6 Q. Okay. Are you aware of anyone of

05:39:20 7 any members of the general public or anyone else

05:39:23 8 besides you that have -- that have done that? Are

20101004kollbergasciil
05:39:26 9 you aware of anybody who's -- who's gone on to the
05:39:29 10 server, you know, put the IP address and used the
05:39:32 11 internet Explorer and -- and gone there to listen
05:39:34 12 to audio files?

05:39:35 13 Do you know of anyone else who has
05:39:37 14 done that, any members of the general public who
05:39:39 15 have done that?

05:39:40 16 A. what do you mean with "general
05:39:41 17 public"?

05:39:42 18 Q. Do you know anybody, anybody who
05:39:43 19 has done that, who has done it the way that you
05:39:45 20 did it on the server?

05:39:46 21 A. I can't tell. I don't see the log
05:39:50 22 files, so I don't know.

□

20101004kollbergasciil

05:39:52 1 Q. But is it -- the way that you're --

05:39:54 2 what your testimony is, so I understand it, was

05:39:58 3 that anybody with a computer and a browser could

05:40:00 4 have done it if they wanted to?

05:40:01 5 A. Yes.

05:40:02 6 Q. And the IP address that you typed

05:40:05 7 in, do you know what the IP address was that you

05:40:08 8 typed -- that you put in, or do you know where we

05:40:10 9 -- that could be found?

05:40:11 10 A. That's in the -- on the hard drive.

05:40:14 11 Q. Okay. And -- and that would be --

05:40:17 12 are there -- are there various IP addresses? I

05:40:19 13 mean, is there -- there's one for each of the

05:40:21 14 seven or eight servers that are registered to IMI.

05:40:24 15 Is that right?

20101004kollbergasciil

05:40:25 16 A. Right.

05:40:25 17 Q. Okay.

05:40:26 18 A. But the phone calls, if I remember

05:40:28 19 correct, haven't been on the Innovative Marketing

05:40:28 20 server.

05:40:32 21 Q. The phone calls were?

05:40:32 22 A. Somewhere else.

□

155

05:40:33 1 Q. Oh, because I -- well, we can see

05:40:35 2 the records. So I think you told me earlier that

05:40:38 3 that was one of the -- that the audio files were

05:40:39 4 from an IMI server.

05:40:41 5 But it's your recollection they're

05:40:43 6 from other place now, not from a server?

20101004kollbergasciil

05:40:45 7 A. I'm not sure. You have to look at
05:40:47 8 the IP addresses. So I think that those servers
05:40:50 9 in India, they have been on a different IP
05:40:53 10 address.

05:40:53 11 Q. And different -- by "different,"
05:40:56 12 you mean a registered -- an IP address that was
05:40:59 13 registered to something else but not to IMI?

05:41:01 14 A. Yes.

05:41:05 15 Q. Okay. To support the -- what your
05:41:12 16 testimony is about the fact that you just -- you
05:41:14 17 know, you just went to an IP address and that
05:41:17 18 there was a link from the IP address to
05:41:19 19 information on the server.

05:41:20 20 Is there any support that you can
05:41:23 21 point me to that -- that backs up the explanation

20101004kollbergasciil
05:41:26 22 that you gave about how it is? Is there any --

□

156

05:41:29 1 anything that you can point me to that would --

05:41:31 2 that would support that that's how it worked, any

05:41:34 3 screen shots or anything at all?

05:41:36 4 A. It's on -- on the hard drive.

05:41:37 5 Q. Okay. And does the material on the

05:41:39 6 hard drive, would it actually illustrate how --

05:41:42 7 how everything that you're telling me about how it

05:41:44 8 worked? I mean, how it worked, that you went to

05:41:47 9 an IP address and that you could without doing

05:41:49 10 anything else link directly to files?

05:41:52 11 A. Yes.

05:41:54 12 Q. When you were talking about using